ALE 系统的链路保护设计*

龙 洋** 罗 宁 黄跃新
（电子科技大学信息所 成都 610054）

【摘要】 ALE 系统介绍了自动链路建立系统中的链路保护设计及其采用的加密算法，是为了解决该系统的信息安全问题，通过大量的实验测试了算法的可靠性。文中通过系统仿真和无保护的系统进行了分析比较，证明了此设计改善了系统的安全性，而且对链路的建立影响很小。

关 键 词 自动链路建立； 链路保护； 保护间隔； 密钥； 加密种子
中图分类号 TN919

1 ALE 系统

短波通信是最原始的无线电通信方式，具有设备简单、机动灵活、抗毁性强等独特优点。但是，由于短波通信的介质—电离层存在较难预报的骚动，而且频率资源有限，使其一度陷入了低谷。随着众多优选频率方法的推出，如采用电离层探测、自适应选频等，形成了具有高度自动化和自适应能力的现代短波通信系统，其核心就是自动链路建立系统（ALE）[1]。ALE 主要包括以下功能：自动信令交换、选呼，自动握手，信道扫描和选择及链路质量分析。因而，采用 ALE 系统，通信设备能够自动选用最佳短波信道进行通信，使系统保持高性能和高效率。

在 ALE 系统具有以上优势的同时，它的开放性也存在以下的弊端：如呼叫和报文等信息易被监听和截获；而且具有恶意的站点还可以盗用别人的地址发起呼叫，造成错误连接，从而引起通信网络的混乱。为了避免上述情况，文献[2]作了链路保护（LP）功能的规定，LP 在 ALE 协议层次中的位置如图 1 所示。

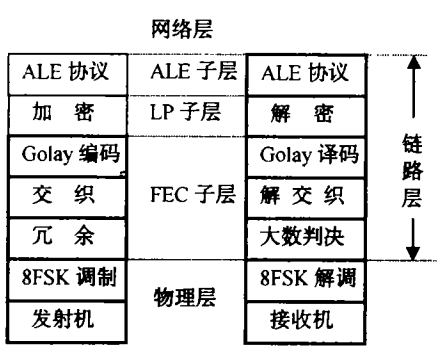

图 1 数据链路层的结构模型

链路保护功能是在数据链路层中实现。通过对 ALE 协议子层传下来的 ALE 字加密，使其全部被扰乱，再通过 FEC 子层发送出去。由于进行了链路保护，只有受保护的站点对接受的信息进行解密才可能成功地建立链路，而那些未经授权的站接收到的只是一阵噪声，自然不能建立链路。从而改善了系统的安全性和通讯的保密性。

在制定链路保护功能时，还根据保护间隔（PI）定义了五种保护级别。而 PI 是收发两站要求达到的时间同步精度。其中，AL-0 是指没采用链路保护功能，而 AL-4 的保护级别最高，它对应的 PI 值也最小。

本文根据 ALE 系统中链路保护设计的原则和要求，重点分析了一种适合于 24 bit 加密算法，并且在此基础上讨论了加入链路保护措施对 ALE 系统连接性能的影响。

2 ALE 系统中的 LP 设计

ALE 子层接收到网络层的信息后，对它们进行处理，形成单位长度为 24 bit 的 ALE 字序列。每个 ALE 字包含了 3 bit 的序头和 21 bit 的数据。其中，序头是 ALE 特定的命令字，用来识别 ALE 字所携带的信息类型。而后面的 21 bit 由三个 7 bit 的 ASCII 字符组成，内容为所呼叫的地址，交换的信令等。发送站使用密钥 KEY 和加密种子 SEED 对 ALE 字加密，密钥由系统指定。而 SEED 是一个时变序列，它包括产生 SEED 的时间（TOD）、所选用的频率和对所发送的 ALE 字的计数。接收站则必须用同样的 KEY

1998 年 4 月 26 日收稿，1998 年 5 月 23 日修改定稿
* 国家“九五”重点科研项目
** 女 24 岁 硕士生

和 SEED 解密才能得到正确的 ALE 字，进而成功地建立链路进行通信。而非法的站点无法获取系统密钥 KEY，同时由于不能获得精确的 TOD，就不能产生正确的 SEED 用于解密，因而也无法干扰或截获正常 ALE 信息交换。

2.1　LP 中的加密算法

在进行链路保护设计时，采用了如图 2 所示的加密算法[3]。加密时，首先将 ALE 字分成三个 8 bit 的 *A*，*B*，*C* 字，在每次加密过程中，把 SEED 和 KEY 与 *A*，*B*，*C* 分别作用，得到的结果，再经过一个扰码表转换。在图 2 中，*O*表示将输入（如待加密的 *A*，*B*，*C* 字）与 SEED 和 KEY 作运算；在每一轮加密中，先将 *A*、*C* 分别与 *B* 及其 SEED 和 KEY 结合运算，得到的结果记为 *A*'、*C*'，再把在这一次过程中未加密的 *B* 和 *A*'、*C*'以及 SEED、KEY 一起进行加密运算。重复以上的加密多次，再把最后得到的输出（加密后的 *A*，*B*，*C*）重新合成 ALE 字，此时的 ALE 字已被全部扰乱。由于，此种算法是可逆的，因而，解密过程便可以此反推。

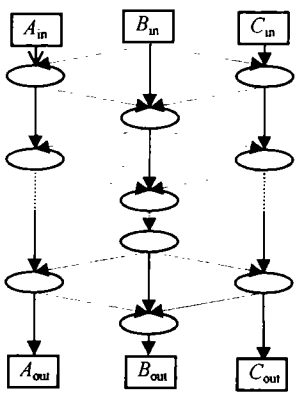

图 2　加密算法的示意图

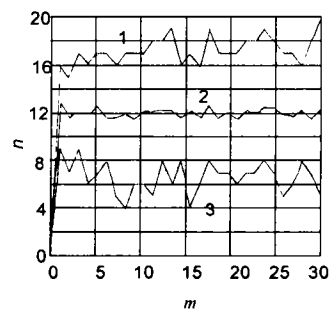

图 3　Seed 中比特对密文影响

2.2 加密算法分析

从上面所述的加密算法可以看出，密文是由 ALE 字与 SEED，KEY 相互作用而得到。ALE 字、SEED 和 KEY 的每比特变化都会引起密文的相应变化，这种变化特性反映了算法的可靠性，为此本文对这种变化特性进行了测试。我们通过改变以上三个对象中的每比特来测试密文的变化。图 3 为测试结果，它反映了 SEED 中的任意比特变化对密文的影响。其中，*m* 为加密次数；*n* 为密文中所改变的比特数目。根据图 3 可得出：只要 SEED 的任意一比特改变，都会引起密文内容的变化。最差的情况是在第二次才开始改变密文，经过五次加密后，密文的变化趋于稳定，即 SEED 中任意比特可引起密文中至少 7 bit 的变动。根据大量测试统计出的平均情况是造成密文的 12 bit 的改变，而引起改变的最大值可达到 19 bit。在测试中，ALE 字和 KEY 中任意一比特改变也会使密文产生类似的变化结果，实验结果在此就不再赘述。因此，采用以上加密算法并经过足够次数（≥5）的加密，根据有限的数据破译出明文的可能性就极小。

2.3　LP 功能对系统性能影响的分析

通过系统仿真，对有保护和无保护状况下建立链路时的性能作了比较。实验采用了单呼单字节地址协议（该协议是 ALE 系统最常用的协议），并用基带的 Watterson 信道模拟器对短波信道进行了仿真[4]。我们选用了两种典型的信道进行了测试：1）高斯白噪声信道（即无多普勒展宽和多径）；2）Poor 信道（根据 CCIR 制定的标准，其多谱勒展宽为 1 Hz，多径延迟为 2 ms）。并对比了三种不同保护等级的系统：1）无保护的 ALE 系统（AL-0 LP）；2）AL-1 LP（PI=60 s）；3）AL-2 LP（PI=2 s）。

图 4、5 中 *P* 为链路建立概率，SNR 为 3kHz 带宽内的信噪比从图中系统仿真结果表明：使用了链路保护，尤其是 AL-2 后，系统成功建立链路的概率和无保护系统相比，仅相差 3~4 个百分点。出现这种微小差距的原因是由于存在错误字同步的问题。在没有链路保护时，FEC 子层从调制解调器接收信息，进行大数判决、解交织和 GOLAY 译码。而 GOLAY 译码仍有很小的错译概率，但是由于 ALE 字有上述

特定的格式，因此，错误的码字即使在 FEC 子层通过，传到 ALE 协议子层时仍会被识别为错字并且拒绝，这样，就不会产生错误的连接。在无保护模式下随机输入码字，GOLAY 码错译的概率为

$$P_{wse}=(1-P_1)P_{pac}=(1-\sum_{i=0}^{48}P_{2,i}P_{3,i})P_{pac}=\left[1-\frac{1}{49}\sum_{i=0}^{48}(1-P_G)^i\right]P_{pac}=$$
$$\left[1-\frac{1}{49}\frac{1-(1-P_G)^{49}}{P_G}\right]P_{pac}\approx 0.005 \tag{1}$$

式中 P_{wse} 为字同步错误概率；P_G 为 GOLAY 解出码字概率；P_{pac} 为任意字通过序头和 ASCII 检查概率；P_1 为在正确字相位前无 GOLAY 错译的概率；$P_{2,I}$ 为在正确字相位前存在 i 个符号的概率；$P_{3,i}$ 为在前 i 个符号无错误 GOLAY 解码的概率。

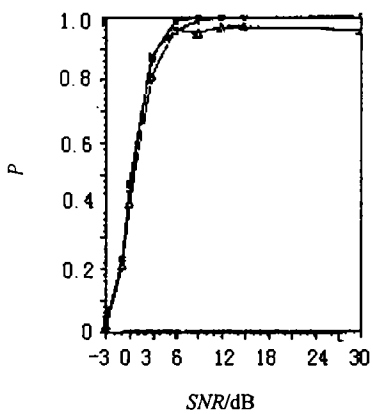

图 4 LP 在 Poor 信道对 ALE 系统性能的影响

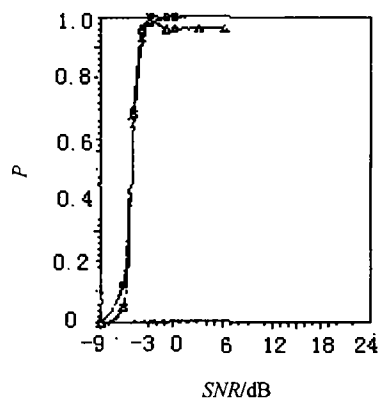

图 5 LP 在高斯信道对 ALE 系统性能的影响

在有保护功能时，码字经过 FEC 子层后，还要通过 LP 解密。由于 ALE 字中没有同步标志，这就给接收站造成了一定难度，主要体现在以下几个方面：

1) 要求准确的 TOD 同步，即通信双方的时钟必须对准；

2) 在获得字同步过程中，不知道发送站的 ALE 字的计数；

3) 在同步前，不能确切知道当前的 ALE 字是属于何字段。

因此，在获得字同步前，接收站需要使用多种 TOD 和码字计数组合的 SEED 解密，并将结果送给 ALE 协议子层判断，确定是否只产生了唯一有效的 ALE 字，以此来确定同步。至此以后，接收站才可能生成确定的 SEED。由于未取得同步前，存在多个解密 SEED，这就造成一些在 FEC 子层侥幸过关的不正确码字，在 LP 子层经过不恰当的 SEED 解密后，成为正确的 ALE 字，这就增大了 P_{wse}，因而系统成功建立链路的概率就相应减小。而且在有 LP 的 ALE 系统中，随着保护级别的提高，PI 值变小，对时间同步的要求也越精确，因而在未同步前，用于凑试的 SEED 数目就越多，则 P_{wse} 也变得更大，链路建立失败的概率相应增大。但由于 Golay 译码的错译概率较低，因而加入链路保护后，造成的连接性能损失并不明显。

3 结 论

由本文的分析和试验结果表明，在系统中加入链路保护功能设计，能够改善系统安全性，并且对系统性能的影响也很小。因此，链路保护技术和本文研讨的加密算法是一种行之有效的 ALE 系统安全控制方案。为了进一步提高保护系统的 ALE 性能，可以加强对调制解调和差错控制技术的研究。

参 考 文 献

1 Military standard interoperability and performance standards for medium and high frequency radio equipment. Philadeplhia: Navy Publications office, 1988

2 Military standard planning and guidance standard for automated control applique for HF radio. Philadeplhia:Navy publications office, 1994

3 Johnson E E, Moore R S. Evaluation of HF Linking Protection. IEEE Milcom, 1993, (1): 328~332

4 Watterson C C, Juroshek J R, Bensema W D. Experimental confirmation of an HF channel model. IEEE Trans on Comm Tech, 1970, COM-18 (6):792~802

Linking Protection Design for ALE System

Long Yang　Luo Ning　Huang Yuexin

(Inst. Of Information Systems, UEST of China Chengdu　610054)

Abstract This paper mainly introduced Linking Protection(LP) scheme and the encryption algorithm adopted in it, which aims at resolving the vulnerability of the automatic link establishment(ALE) system's security. The algorithm's realiability is proved by lots of teses; And the performance of LP scheme is analyed by simulating. The results of the simulation prove that the scheme enchances the system's security, however duing to the word synchronization, it affects the performance a little .

Key words automatic link establishment; linking protection; protection interval; encryption key; seed

• 科研成果介绍 •

多层薄膜厚度及成分的无损检测技术

主研人员　眭松山　梅学明　魏　军　李学为　史　青

跟踪国际无损检测技术，正确合理地设计了求解 1~5 层多层薄膜材料厚度与成分含量的整套理论计算式，重要参数的运算比较与筛选，用 C/C++语言设计成同时测算膜厚与组份的新方法、实用软件和用户界面。

该成果与国外同类专用软件技术比较有如下优点：能适应于不同的 X 光管发射源和仪器条件，具有通用性；能揭示中间运算过程和各种激发机理模式；脱机应用范围广，操作简便，输出结果和运算速度与国外同类专用软件相当。该技术可应用于科学研究和综合技术服务业，是目前国内外军用或民用薄膜材料生产、研究中不可缺少的重要支撑技术。

•科　卞•